Les atteintes aux systèmes informatisés de données

Dans le cadre des cours de M. FERRY et de M. NEVEU

mardi, 1er mars 2005 / **Nguyen Trinh Thiet** , / **Haja Rakotozafy** / Politologue - Juriste des NTIC

L'informatique est une Science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications dans les domaines technique, économique et social (définition approuvée par l'Académie française).

Les systèmes informatisés des données ou AIS (Automated Information System) : C'est une expression désignant tous les équipements (de nature matérielle, logicielle, ou « firmware«) permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission, ou la réception de données. (*Lexique)*

Tout cela est prévu par le Code pénal au chapitre III (art. 323-1 à 323-3-1). Voir annexe.

Loi GODFRAIN, Loi n° 88-19 du 5 Janvier 1988 relative à la fraude informatique : Le 5 janvier 1988, le législateur en est parfaitement conscient. Aujourd'hui, 17 ans après l'entrée en vigueur de la loi, et après les révolutions technologiques que nous avons connues, il est légitime de se demander si la loi est encore applicable et si elle n'a pas totalement versé dans l'obsolescence.

Le système

Les infractions définies par la loi du 5 janvier 1988 sont relatives aux atteintes aux « systèmes de traitement automatisé de données « , « STAD ». Une définition en avait été proposée lors des débats parlementaires, mais elle n'a pas été retenue dans le souci de ne pas lier l'incrimination à un état trop passager de la technique.

Les tribunaux ont aujourd'hui de cette notion une conception large : le réseau France Telecom est un système, le réseau Carte bancaire aussi (Trib. cor. Paris, 25 fev. 2000), un disque dur (Cour d'appel de Douai, 7 oct. 1992), un radiotéléphone (Cour d'appel de Paris, 18 nov. 1992), un ordinateur isolé, un réseau ...

On peut se demander jusqu'ou la notion de « système « peut être retenue : un petit ordinateur portable, un PDA, téléphone portable, une montre pourquoi pas aussi ?

Exigence d'un dispositif de sécurité

Si le système existe et si son objet est bien le traitement automatisé de données, se pose la question de sa protection. La jurisprudence apporte ici une réponse négative, en ne retenant pas l'existence

d'un dispositif de sécurité comme une condition préalable à la réalisation de l'infraction. Autrement dit, un système peut parfaitement faire l'objet d'un accès frauduleux quand bien même il ne disposerait d'aucun mécanisme de sécurité.

I. Les actions sur le plan juridique

A- Les responsabilités pénales

La loi Godfrain du 8 janvier 1988, bien qu'élaborée à une époque où on ne parlait pas encore d'Internet et dont les dispositions ont été reprises par le Code pénal dans un chapitre intitulé « Des atteintes au système de traitement automatisé de données « , permet de sanctionner toutes les intrusions non autorisées dans un système informatique. Les sanctions prévues varient selon que l'intrusion a eu ou non une incidence sur le système en cause.

1. Les atteintes simples

L'article L.323-1 du Nouveau code pénal prévoit que « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende « . Ces systèmes comprennent, entre autre, les sites web. Actuellement les sanctions se voient connaître un alourdissement conséquent. Elles peuvent aller jusqu'à 3 ans d'emprisonnement et 45 000 euros d'amende (art. L. 323-1 du nouveau code pénal) [1].

a) Accès frauduleux

La Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 que « l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication« .

Quid, pourtant, si le système n'est pas protégé ? La Cour d'appel de Paris, dans un arrêt en date du 30 octobre 2002 , a jugé que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible. Elle a, ainsi, reformé le jugement du Tribunal de grande instance de Paris, qui avait estimait que l'existence des failles de sécurité ne constituait « en aucun cas une excuse ou un prétexte pour le prévenu d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale « . En effet, l'article 226-17 du Code Pénal réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment d'empêcher qu'elles ne soient communiquées à des tiers non-autorisés. L'incrimination vise notamment les « *white hackers*« ou, plus généralement les « curieux« , dépourvus d'intention de nuire ou de modifier le système (il s'agit ici de l'affaire TATI, domaine que nous allons creuser un peu plus loin). L'incrimination suppose que la personne qui accède au système y accède « *frauduleusement*« , à savoir :

- volontairement (l’accès n’est pas accidentel)

- et sans disposer d’aucun droit ni d’aucune autorisation afin d’accéder au système.

Dans une décision du 4 décembre 1992, la Cour d’appel de Paris a écarté les délits d’accès et de maintien dans un système de traitement automatisé de données informatiques en constatant que l’appropriation d’un code d’accès avait pu être le résultat d’une erreur de manipulation sur les fichiers, cette circonstance excluant le caractère intentionnel exigé par la loi.

b) Le maintien frauduleux

La loi incrimine également le maintien frauduleux ou irrégulier dans un système de traitement automatisé de données de la part de celui qui y est entré par inadvertance ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement (Cour d’appel de Paris, jugement du 5 avril 1994 précité).

Quant à l’élément intentionnel de cette infraction, la doctrine et la jurisprudence s’accordent à admettre que l’adverbe « frauduleusement « n’est pas le dol général de l’attitude volontaire, ni le dol très spécial de l’intention de nuire, mais la conscience chez le délinquant que l’accès ou le maintien ne lui était pas autorisé.

2. Les atteintes avec dommages

L’alinéa 2 de l’article 323-1 du nouveau Code pénal prévoit un renforcement des sanctions, lorsque l’intrusion et le maintien frauduleux ont certaines conséquences :

« Lorsqu’il en résulte soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d’emprisonnement et de 30 000 euros d’amende «

Ne sont concernées par cet article que les altérations involontaires. L’entrave volontaire au système ou l’entrave volontaire aux données sont visés par les articles 323-2 et 323-3 du nouveau Code pénal.

3. Les entraves volontaires au système ou aux données s’y trouvant

L’article 323-2 du Nouveau Code pénal définit l’entrave volontaire au système comme « Le fait d’entraver ou de fausser le fonctionnement d’un système de traitement automatisé de données « . Le peine encourue est de trois ans d’emprisonnement et de 45.000 euros d’amende. Cette infraction vise, notamment, l’introduction des programmes susceptibles d’entraîner une perturbation au système, tels que les virus, les bombes logiques etc.

L'article 323-3 du Nouveau Code pénal sanctionne, par ailleurs, l'introduction, la suppression ou la modification frauduleuses de données dans un système informatique. Les applications illicites visées par cet article sont nombreuses. Elles peuvent aller de la réduction du prix des marchandises sur un site de commerce électronique, la modification ou la suppression du contenu des bases de données à la modification du statut fiscal de l'entreprise.

En tout cas, ces agissements sont susceptibles d'entraîner une perte financière considérable au sein de l'entreprise.

B- La responsabilité civile délictuelle et contractuelle

1. La responsabilité civile délictuelle

Le droit commun de la responsabilité civile délictuelle est fondée sur la nation de la faute au sens de l'article 1382 du Code civil. Elle nécessite une faute, un dommage et un lien de causalité entre les deux. La faute consiste ici en une intrusion dans un système informatique à l'insu de son utilisateur. Quant au dommage, il faut savoir s'il y a eu une perte et/ou une altération des informations contenues dans le site ou si le pirate a communiqué les données personnelles s'y trouvant à des tiers. Enfin, le lien de causalité entre la faute et le dommage doit être clairement établi.

Quid, pourtant, si le pirate n'est pas de nationalité française ou s'il opère de l'étranger ? La question qui se pose, dans ce cas, est celle de la compétence judiciaire internationale et de la loi applicable.

En droit français, le tribunal compétent pour juger un litige international est, en principe, celui du domicile du défendeur, à moins que le demandeur, s'il est français, ne souhaite invoquer le privilège de juridiction des articles 14 et 15 du Code civil. Or, ce dernier privilège est interdit dans le cadre de la Communauté européenne par la Convention de Bruxelles de 1973, devenue en 2000 un règlement « concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale « .

S'agissant d'un délit ou d'un quasi-délit, les articles 5§3 de la Convention de Bruxelles et du règlement 44/2001 précité, posent une règle de compétence spéciale en faveur du tribunal où le fait dommageable s'est produit ou risque de se produire. Ce lieu peut être aussi bien celui où le dommage est survenu qui celui de l'événement causal qui est à l'origine de ce dommage (CJCE, 30 novembre 1976, affaire C-21/76, Mines de potasse d'Alsace : Rec. CJCE, p. 1735).

Dans le cas où le dommage, causé par l'intrusion, serait survenu au sein du système informatique d'une société domiciliée en France, les juridictions françaises seraient sans doute compétentes pour juger le litige.

Quant à la loi applicable, le juge applique, de manière générale la lex loci delicti, c'est à dire la loi où le fait dommageable s'est produit. La Cour de Cassation a jugé que le lieu où le fait dommageable s'est produit s'entend aussi bien de celui du fait générateur du dommage que du lieu de réalisation de ce dernier (Cass. 1re civ., 14 janvier 1997, D. 1997, p.177).

2. La responsabilité civile contractuelle

Il est possible, en effet, d'engager la responsabilité civile contractuelle de l'héberger du site. Pour cela, il faudrait examiner les clauses contenues dans le contrat d'hébergement concernant notamment la sécurité du site et la mise en place de systèmes informatiques de protection contre toute forme d'intrusion. Il faudrait aussi qualifier cette obligation de l'héberger : s'agit-il d'une obligation de résultat ou de moyens ? Dans la plus part de cas, il ne pourra s'agir que d'une obligation de moyens qui aura pour effet de contraindre le prestataire d'apporter la preuve qu'il n'a pas manqué aux obligations normales qui lui incombaient, en cas d'intrusion informatique non autorisée.

II. La Protection du système

La protection du système est-elle une condition d'application de l'article 323-1, alinéa 1er, du nouveau Code pénal ? A priori, une réponse négative s'impose. La protection du système n'est pas une condition de l'incrimination.

Dans une décision du 5 avril 1994, la Cour d'appel de Paris a précisé que « pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection...« . La Cour a encore précisé qu'il suffit, pour que l'accès ou le maintien soit « punissable« que « le maître du système ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées« .

De sorte que, contrairement à une idée répandue, l'absence de système de sécurité, voire une réelle facilité d'accès ne met pas obstacle à l'infraction, sauf si cet accès est accidentel et que la personne qui accède au système ne cherche pas à s'y maintenir volontairement sans droit.

A- L'obligation de sécurité des données personnelles

Selon les termes de l'article 29 de la loi du 6 janvier 1978 dite « *Informatique et Libertés*« :

« Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. «

Il s'agit d'une « *obligation de sécurité des données personnelles*« , dont le non-respect est sanctionné par l'article 226-17 de nouveau Code pénal :

« Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et

notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 2.000.000 francs d'amende. « .

B- L'affaire TATI

Le 30 octobre 2002, dans une affaire célèbre opposant la société TATI à un journaliste, spécialisé en informatique, administrateur du site internet KITETOA.COM, la Cour d'appel de Paris est venue nuancer sa jurisprudence antérieure. Sur appel à l'encontre du jugement de condamnation du Tribunal de grande instance de Paris en date du 13 février 2002, le prévenu a été relaxé. La Cour a considéré qu'on ne pouvait pas reprocher à un internaute d'accéder ou de se maintenir dans les parties d'un site accessible par la simple utilisation d'un logiciel de navigation, et que *« ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès (...). La détermination du caractère confidentiel et des mesures nécessaires à l'indication et à la protection de cette confidentialité relevant de l'initiative de l'exploitant du site ou de son mandataire* « .

Voici le rappel des faits :

Il s'agit d'une affaire qui mettait en exergue le problème d'atteintes aux systèmes informatisés de données. CHAMPAGNE Antoine, un journaliste informatique, a pu accéder dans le répertoire-clients de Tati et affirme l'avoir accidentellement fait en utilisant les simples fonctionnalités habituelles de Navigator Enterprise Server de TATI.fr. Il signale cette faille de sécurité à ce dernier. Par la suite, il *est poursuivi pour avoir à Paris et en tout cas sur le territoire national, entre novembre 1997 et novembre 2000 et en tout cas depuis temps non prescrit, accédé ou s'être maintenu, frauduleusement, dans un système de traitement automatisé de données, en l'espèce le système de traitement automatisé de données de la SA TATI.*

Le TGI de Paris, par jugement contradictoire, a déclaré CHAMPAGNE Antoine, coupable d'ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES, de novembre 1997 à novembre 2000, à Paris, infraction prévue par l'article 323-1 AL.1 du Code pénal et réprimée par les articles 323-1 AL.1, 323-5 du Code pénal et, en application de ces articles, l'a condamné à une amende délictuelle de 1.000 Euros avec sursis.

Le Procureur Général près de la Cour d'Appel de Paris a interjeté appel, le 03 Avril 2002 contre ledit jugement déclarant coupable Monsieur CHAMPAGNE Antoine.

Finalement le juge d'appel, a relaxé le journaliste sous prétexte qu'*il ne peut être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ; que même s'agissant de données nominatives, l'internaute y accédant dans de telles conditions ne peut inférer de leur seule nature qu'elles ne sont pas publiées avec l'accord des intéressés, et ne peut dès lors être considéré comme ayant accédé ou s'étant maintenu frauduleusement dans cette partie du système automatisé de traitement de données, la*

détermination du caractère confidentiel (en l'espèce non discuté mais qui n'a donné lieu à aucune utilisation en pratique préjudiciable) et des mesures nécessaires à l'indication et à la protection de cette confidentialité relevant de l'initiative de l'exploitant du site ou de son mandataire ; que dès lors les accès et maintien d'Antoine CHAMPAGNE dans des parties nominatives du site TATI ne peuvent être qualifiés de frauduleux, et qu'il convient de déclarer le prévenu non coupable des faits qui lui sont reprochés et de le renvoyer des fins de la poursuite... En un mot, le problème juridique soulevé par le juge repose sur le fait que la partie plaignante a manqué aux obligations légales de protections de données.

Par extension, on peut dire que cette affaire met en l'application l'adage nemo pluri juris nullis turpitudis (nul ne peut se prévaloir de sa propre turpitude). Cette jurisprudence conduit à exiger la mise en place d'une protection adaptée du système ou, lorsqu'il s'agit d'un serveur Internet, de codes et mots de passe en restreignant utilement l'accès. En l'absence de toute mesure de protection, l'accès ou le maintien pourrait ne pas être considéré comme « *frauduleux*« au sens de la loi.

Mais quid des abus que les esprits malveillants peuvent tirer de ce manquement aux obligations de protection ? A notre avis l'affaire semble en suspens puisqu'il n'est pas impossible qu'elle soit portée devant les juges de la cassation.

Par Hajanirina RAKOTOZAFI et Trinh Thiet N'GUYEN

ANNEXE

Annexe 1 :

ARRÊT DU 30 OCTOBRE 2002
COUR D'APPEL DE PARIS 12ème CHAMBRE, SECTION A

Prononcé publiquement le MERCREDI 30 OCTOBRE 2002, par la 12ème CHAMBRE DES APPELS CORRECTIONNELS, SECTION A,

Sur appel d'un jugement du TRIBUNAL DE GRANDE INSTANCE DE PARIS - 13ème CHAMBRE du 13 FEVRIER 2002, (P0113590097).

PARTIES EN CAUSE DEVANT LA COUR :

CHAMPAGNE Antoine,
de nationalité française, marié, journaliste,
Prévenu, comparant, libre, intimé,

Assisté de Maître ITEANU Olivier, Avocat au Barreau de PARIS (D 1380)
ALIAS : KITETOA

LE MINISTÈRE PUBLIC : Appelant,

LA SOCIETE TATI ,
4, Boulevard Rochechouart - 75018 PARIS
Partie civile, non appelante
Représentée par Maître GRABLI Elisabeth, Avocat au Barreau de PARIS (D 367)

COMPOSITION DE LA COUR,

lors des débats et du délibéré :

Président : Monsieur MERIDIAS,
Conseillers : Monsieur BERAUD, Madame BIGOURDAN,
GREFFIER : Madame CAPY, lors des débats et au prononcé de l'arrêt,
MINISTÈRE PUBLIC : représenté lors des débats, par Monsieur MADRANGES, Avocat Général et au prononcé de l'arrêt, par Madame CATTA Avocat Général .

RAPPEL DE LA PROCÉDURE :

LA PREVENTION :

CHAMPAGNE Antoine, est poursuivi pour avoir à Paris et en tout cas sur le territoire national, entre novembre 1997 et novembre 2000 et en tout cas depuis temps non prescrit, accédé ou s'être maintenu, frauduleusement, dans un système de traitement automatisé de données, en l'espèce le système de traitement automatisé de données de la SA TATI.

LE JUGEMENT :

Le Tribunal, par jugement contradictoire, a déclaré CHAMPAGNE Antoine, coupable d'ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES, de novembre 1997 à novembre 2000, à Paris, infraction prévue par l'article 323-1 AL.1 du Code pénal et réprimée par les articles 323-1 AL.1, 323-5 du Code pénal

et, en application de ces articles, l'a condamné à

Une Amende délictuelle de 1.000 Euros avec sursis,

Déclaré recevable la constitution de partie civile de la Société TATI, mais l'a débouté de sa demande.

L'APPEL :

Appel a été interjeté par :
Le Procureur Général, le 03 Avril 2002 contre Monsieur CHAMPAGNE Antoine,

DÉROULEMENT DES DÉBATS :

A l'audience publique du 25 SEPTEMBRE 2002, le président a constaté l'identité du prévenu ;

Monsieur MADRANGES, Avocat Général, a sommairement indiqué les motifs de l'appel interjeté par le Procureur Général ;

ONT ETE ENTENDUS
Monsieur MERIDIAS, Président, en son rapport ;
CHAMPAGNE Antoine, en ses explications ;
Maître GRABLI, Avocat de la partie civile en sa plaidoirie ;
Monsieur MADRANGES, Avocat Général en ses réquisitions ;
Maître ITEANU, Avocat en sa plaidoirie ;
CHAMPAGNE Antoine, a eu la parole en dernier.

Le Président a ensuite averti les parties que l'arrêt serait prononcé le 30 OCTOBRE 2002 et audit jour le dispositif a été lu par l'un des magistrats ayant participé aux débats et au délibéré, conformément aux dispositions de l'article 485 dernier alinéa du Code de Procédure Pénale ;

DÉCISION :

Rendue après en avoir délibéré conformément à la loi,

Considérant que le Procureur Général près la Cour d'Appel de Paris a régulièrement fait appel du jugement susvisé, par lequel Antoine CHAMPAGNE a été déclaré coupable d'accès ou maintien frauduleux dans le système de traitement automatisé des données de la société TATI entre novembre 1997 et novembre 2000 à Paris, et condamné de ce chef à une amende de 1.000 euros avec sursis, la société TATI qui s'était portée partie civile étant reçue en ses demandes mais en étant déboutée aux motifs de ses carences et négligences et du fait que l'éventuel préjudice n'aurait pu être subi que par d'autres ;

Considérant qu'il est constant et non discuté, qu'au moins de juin 1999 à juin 2000, Antoine CHAMPAGNE, qui est journaliste en informatique et administrateur d'un site Internet intitulé KITETOA.COM, sur lequel il dénonce notamment les insuffisances des protections des données

contenues par les systèmes de traitement automatisé des informations reliés à Internet, a plusieurs fois pénétré le site Internet de la société TATI, assez profondément pour y parvenir au répertoire des fichiers de données nominatives puis à ces fichiers eux-mêmes, et ce par la seule utilisation des fonctionnalités du navigateur grand public NETSCAPE ; qu'à la suite de son premier accès en 1999 il a envoyé un message de mise en garde, resté sans réponse, à l'exploitant du site ; qu'ayant à nouveaui tenté l'expérience et ayant obtenu le même résultat en juin 2000, il a réitéré son message, envoi dont il est résulté que très rapidement les données des fichiers nominatifs ont cessé d'être accessibles à la diligence de la société OGILVY qui avait repris l'exploitation du site pour le compte de la société TATI depuis la fin juin 1999 et que quelques mois plus tard, en octobre 1999, le site avait pu être entièrement sécurisé, cependant que néammoins, en novembre 2000, la revue Newbiz publiait, en pages 19 et suivantes, un article sur la perméabilité du site TATI, y compris des photos d'écrans affichant des données personnelles mais illisibles ;

Considérant que, comme l'appelant le soutient à bon droit dans ses réquisitions écrites d'appel aux fins de relaxe, il ne peut être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ; que même s'agissant de données nominatives, l'internaute y accédant dans de telles conditions ne peut inférer de leur seule nature qu'elles ne sont pas publiées avec l'accord des intéressés, et ne peut dès lors être considéré comme ayant accédé ou s'étant maintenu frauduleusement dans cette partie du système automatisé de traitement de données, la détermination du caractère confidentiel (en l'espèce non discuté mais qui n'a donné lieu à aucune utilisation en pratique préjudiciable) et des mesures nécessaires à l'indication et à la protection de cette confidentialité relevant de l'initiative de l'exploitant du site ou de son mandataire ; que dès lors les accès et maintien d'Antoine CHAMPAGNE dans des parties nominatives du site TATI ne peuvent être qualifiés de frauduleux, et qu'il convient de déclarer le prévenu non coupable des faits qui lui sont reprochés et de le renvoyer des fins de la poursuite ;

PAR CES MOTIFS

LA COUR,

Statuant publiquement et contradictoirement,

Reçoit le Ministère Public en son appel,

Réformant le jugement,

Déclare Antoine CHAMPAGNE non coupable des faits visés à la prévention et le renvoie des fins de la poursuite,

Reçoit la Société TATI en sa constitution de partie civile, mais la trouve mal fondée en ses demandes, et l'en déboute.

LE GREFFIER, LE PRESIDENT

G. CAPY M. MERIDIAS

Annexe 2

PARQUET GENERAL DE LA COUR D'APPEL DE PARIS 12ème CHAMBRE DES APPELS CORRECTIONNELS

Ministère public : Etienne Madranges

R E Q U I S I T I O N S aux fins de relaxe

Le Procureur Général soussigné,

Vu la procédure et les éléments suivants :

La personne poursuivie

CHAMPAGNE Antoine né le 17 novembre 1967 à Paris (16ème) journaliste

libre

prévenu d' accès et maintien frauduleux dans un système de traitement automatisé de données

Les faits

Découverte par un journaliste d'une faille dans la sécurité d'un serveur informatique

En juin 1999, Antoine CHAMPAGNE, journaliste, et administrateur d'un site internet intitulé KITETOA.COM, constatait, à l'occasion d'un accès au site www.tati.fr, mis en place par la société TATI, qu'il pouvait prendre connaissance d'un répertoire-clients de cette entreprise, et ce, sans aucune manipulation frauduleuse, l'accès à un tel répertoire étant la conséquence d'une faille dans la sécurité du serveur TATI. Manifestement, les techniciens ayant organisé ce serveur ou la banque de données TATI n'avaient pas verrouillé le système pour le rendre imperméable à des intrusions étrangères.

Action de ce journaliste

Antoine CHAMPAGNE prévenait les administrateurs du site TATI. Mais il constatait, en mai 2000, soit près d'un an plus tard, que les failles détectées existaient toujours, malgré ses mises en garde. Il publiait dès lors sur son propre site KITETOA un article relatant la faille du système de traitement automatisé de données (STAD, et ainsi désigné dans la suite de ce réquisitoire) de TATI.

La plainte

En octobre 2000, un autre journaliste, Stéphane BARGE, prenait connaissance du contenu du site KITETOA, et donc des informations révélées par Antoine CHAMPAGNE, et il publiait un article dans un magazine spécialisé.

Les dirigeants de TATI lisaient cet article, et décidaient de déposer plainte, estimant avoir été victimes d'une intrusion illicite dans leur STAD.

La procédure

L'enquête

Une enquête préliminaire était diligentée par la Brigade BEFTI de la DRPJ de Paris, service spécialisé dans les enquêtes sur l'informatique et internet.

Interrogé, Antoine CHAMPAGNE expliquait qu'il ne s'était pas introduit frauduleusement dans le STAD de TATI, mais qu'il était parvenu à lire les données du répertoire-clients, et à télécharger certains documents par le simple usage des fonctionnalités du logiciel NETSCAPE, dans sa version grand public, accessible à tous. Il lui avait donc suffi de cliquer sur les icônes que NETSCAPE fait apparaîtresur l'écran, sans aucune fraude.

Dans la conclusion de son procès verbal de synthèse, l'Officier de Police Judiciaire OPJ ayant procédé à l'enquête écrivait qu' Antoine CHAMPAGNE était l'auteur de plusieurs accès et maintiens frauduleuxsur le STAD deTATI.

La citation

Antoine CHAMPAGNE était cité par le Parquet de Paris à comparaître devant le tribunal correctionnel, pour avoir : à Paris, entre novembre 1997 et novembre 2000, accédé ou s'être maintenu, frauduleusement, dans un système automatisé de données, en l'espèce le système de traitement automatisé de données de la SA TATI.

Le jugement

Lors de l'audience du 23 janvier 2002, Antoine CHAMPAGNE niait toute fraude et sollicitait sa relaxe. TATI demandait la réparation de son préjudice.

Par jugement en date du 13 février 2002, le tribunal correctionnel de Paris (13ème chambre) déclarait Antoine CHAMPAGNE coupable d'accès frauduleux dans un système de traitement automatisé de données, et le condamnait à une amende de 1.000 euros avec sursis. Le tribunal déboutait la partie civile, TATI, de sa demande, en application de la règle « nemo auditur« (nul ne peut alléguer sa propre turpitude).

Estimant bénéficier d'une sanction de principe, modique quant au quantum, Antoine CHAMPAGNE ne relevait pas appel. TATI, constatant sans doute que sa responsabilité pénale pouvait elle aussi être envisagée, n'engageait pas de recours non plus.

L'appel du parquet général de Paris

Le 3 avril 2002, le parquet général relevait appel du jugement. Il faisait signifier son appel par huissier.

Cet appel est recevable, pour être intervenu dans le délai et selon les formes prévus par l'article 505 du code de procédure pénale.

Cet appel a pour objet de faire réformer par la Cour la décision des premiers juges, de solliciter la relaxe du prévenu, en suscitant la mise en oeuvre d'une jurisprudence mettant fin à l'insécurité juridique qui pourrait résulter d'interprétations erronées des dispositions pénales relatives à l'informatique.

L'infraction soumise à l'appréciation de la Cour

Antoine CHAMPAGNE est poursuivi pour avoir commis le délit prévu par le premier alinéa de l'article 323-1 du code pénal, qui dispose :

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15.000 euros d'amende.

Pour que l'infraction soit constituée, il faut donc :

que soit concerné un STAD ; c'est le cas en l'espèce, s'agissant d'un système de données exploité par TATI par le biais d'un serveur externe

qu'il y ait accès, ou maintien, dans ce système

que cet accès et ce maintien soient frauduleux

On peut déduire de cette lecture qu'il faut que le système soit forcé, ou à tout le moins que l'intrusion soit irrégulière.

Discussion

Le contenu du jugement

Le jugement contient des éléments qui peuvent apparaître contradictoires.

En début de motivation, il énonce :

« Attendu qu'aucun élément de la procédure ne démontre que le prévenu ait fait usage pour avoir accès au fichier clients ci-dessus d'autres manipulations que celles qu'il a décrites qu'il résulte de ces éléments que le fichier litigieux était accessible par la seule utilisation des fonctionnalités du navigateur NETSCAPE« .

En fin de motivation, le jugement énonce qu' Antoine CHAMPAGNE « avait nécessairement conscience que son accès et son maintien dans le site de la société TATI étaient frauduleux« .

Dans le dispositif, le Tribunal, oubliant la notion et l'incrimination de maintien dans le STAD, condamne pour accès dans un SATD.

Il n'y a en conséquence pas concordance entre les motifs et le dispositif, et il y a une contradiction à l'intérieur des motifs, puisqu'une manipulation considérée comme licite devient in fine une méthode frauduleuse par la seule conscience que l'on a d'avoir découvert une chose à laquelle on n'a normalement pas accès.

Le fond de l'affaire

Le comportement de la partie civile

La société TATI a mis en place ou fait mettre en place un serveur sans s'assurer que les données confidentielles concernant ses clients étaient protégées. Ses dirigeants ont ainsi commis l'infraction prévue par l'article 226-17 du code pénal, qui dispose : Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende.

Cette infraction, plus grave que celle reprochée à Antoine CHAMPAGNE, n'a, en l'absence de plainte, pas fait l'objet de poursuites de la part du ministère public.

Cette carence de la société TATI ne saurait cependant constituer une excuse ou une circonstance atténuant la responsabilité pénale de ceux qui chercheraient, par des moyens frauduleux, à accéder au STAD litigieux.

Dans ses conclusions devant le tribunal, la partie civile a fait valoir que le fait par Antoine CHAMPAGNE de se maintenir sans droit dans le système était constitutif d'une infraction, citant un arrêt rendu par la Cour d'appel de Douai le 7 octobre 1992, qui avait décidé que le délit était constitué dès lors que l'auteur avait conscience de ce qu'il accédait ou se maintenait sans droit dans le système.

L'accès et le maintien ont-ils été frauduleux ?

Il n'est pas contesté qu' Antoine CHAMPAGNE a eu accès aux données contenues dans le serveur exploité par TATI. Le point essentiel est de déterminer si le journaliste a utilisé des moyens frauduleux.

Le tribunal, dans son jugement, a déjà partiellement répondu à cette question, en affirmant qu' Antoine CHAMPAGNE n'avait eu accès aux données du répertoire-clients de TATI qu'en utilisant le seul navigateur NETSCAPE et ses fonctionnalités habituelles.

En l'espèce, il apparaît clairement que le journaliste n'a utilisé aucune méthode de piratage. Il n'a pas cherché à « craquer« , tel un « hacker« (pour reprendre des expressions courantes dans ce domaine). Il n'est même pas établi qu'il ait cherché à tricher, à utiliser de façon abusive des fonctionnalités d'un logiciel en vente libre.

Il a utilisé les fonctionnalités d'origine du logiciel NETSCAPE, qui est, avec Microsoft Internet Explorer, l'un des deux grands logiciels de navigation sur internet, se contentant de cliquer sur les icônes apparaissant sur son écran.

Une telle manipulation est accessible à tout internaute averti, non ingénieur, non technicien, non spécialisé, mais qui sait lire un mode d'emploi. Le caractère frauduleux de cette manipulation n'est pas établi par la procédure.

Quant au fait de télécharger certaines données, cela n'est pas reproché au prévenu. D'ailleurs, il n'y a pas d'intention de nuire, puisque le journaliste a copié des « écrans« dans le seul but de conforter la véracité de ses tests, et non pour nuire à TATI, ses clients, sa renommée.

Il s'agit en définitive de décider si l'accès par des moyens légaux au contenu d'un système dont on n'est ni le créateur, ni le détenteur ni l'exploitant, dans un but de curiosité, ou dans le souci d'en tester la fiabilité, surtout quand on est journaliste d'investigation, est punissable par la seule

conscience que l’on a d’y être parvenu sans piratage, volontairement ou involontairement.

La réponse doit à l’évidence être négative.

Antoine CHAMPAGNE n’a pas agi par malveillance. Il est établi qu’il a prévenu les administrateurs du serveur TATI. Le prévenu a d’ailleurs fourni les documents attestant de l’échange de courriers électroniques entre lui et ces administrateurs.

Lorsqu’une base de données est, par la faute de celui qui l’exploite, en accès libre par le biais de l’utilisation d’un logiciel de navigation grand public ne nécessitant pas de connaissances particulières ou de manipulations à la limite du piratage, le seul fait d’en prendre connaissance, et même pour un journaliste, un testeur, mandaté ou non, d’en réaliser une copie (par simple copie d’écran, ce qui a été le cas) sans intention malveillante, sans révélations permettant d’éventuelles identifications (de codes, de chiffres comptables, de clients d’une société par exemple...), ne saurait constituer une infraction.

Il en irait autrement si l’internaute « testeur« forçait un passage, réalisait un accès à un STAD par une manipulation de piratage nécessairement volontaire, intentionnelle, frauduleuse.

L’élément intentionnel et la volonté de nuire sont d’autant moins établis qu’ Antoine CHAMPAGNE a averti les responsables de la situation défectueuse et des failles découvertes.

Il semble inenvisageable d’instaurer une jurisprudence répressive dont il résulterait une véritable insécurité permanente, juridique et judiciaire, pour les internautes, certes avisés, mais de bonne foi, qui découvrent les failles de systèmes informatiques manifestement non sécurisés.

La solution dans les travaux préparatoires du Parlement

N’était-ce d’ailleurs pas la volonté du législateur, puisqu’on peut lire, dans l’un des rapports établis lors de la discussion devant le Sénat du texte de loi réprimant les fraudes informatiques, et concernant la prévention objet du présent dossier, le paragraphe suivant, qui contient les éléments de réponse au cas d’espèce :

« On notera toutefois que, dans sa rédaction actuelle, cette disposition est applicable à toutes les intrusions dans un système, sous réserve de l’appréciation souveraine que le juge portera sur le caractère frauduleux de l’accès. Le rapporteur a précisé qu’il convenait de considérer qu’il y aura accès frauduleux dès lors qu’on cherchera à s’introduire indûment dans un système protégé par un dispositif de sécurité et le Garde des Sceaux a souligné au cours des débats que le droit pénal ne doit pas compenser l’insuffisance ou la défaillance des mesures de sécurité. Cette exigence d’une protection du système pour que l’infraction soit constituée paraît raisonnable ; on regrettera, là encore, qu’elle ne soit pas explicitement inscrite dans la loi.« .

Réquisitions aux fins d’infirmation et de relaxe

Requiert qu'il plaise à la Cour

Vu les articles 496 et suivants, 515 et 516 du code de procédure pénale, 323-1 du code pénal

en la forme, déclarer l'appel recevable

au fond, faisant droit aux présentes réquisitions, infirmer le jugement du tribunal correctionnel de Paris, et prononcer la relaxe du prévenu.

Fait au Parquet Général de Paris, le 12 juin 2002

Le Procureur général

http://www.kitetoa.com/Pages/Textes...

[1] **Article 323-1** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.*(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002 ; Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)*
